Computer Engineering and Applications Vol. 6, No. 1, February 2017

Least Significant Braille Method in Steganography Using Digital Image Media For Security Message

Megah Mulya[(1)], Zikry Sugiwa[(2)]

(1) Department of Informatics, Faculty of Computer Science, Universitas Sriwijaya
megahmulya@yahoo.com
(2) Department of Informatics, Faculty of Computer Science, Universitas Sriwijaya
Zikry14sugiwa@yahoo.co.id

ABSTRACT

Confidentiality of the message or the information is the most important and essential. It is very influential on the party who has the valuable message when they want to exchange messages on others. To keep the message is not known to others, the necessary security on the message. Steganography is one technique for providing security to the message. Steganography is a technique to hide messages in a medium, such as pictures, sounds and video. Steganographic technique used in this study is the Least Significant Braille (LSBraille). This technique makes use of human vision in the message on the bit value was not significant. This study focuses on how much resistance level stego image to various image processes and measure results accuracy Peak Signal to Noise Ratio (PSNR). From the result of the insertion of a secret message, that the level of resistance stego image is not resistant to digital image processing. The result of the calculation of PSNR value obtained from experiments on all data samples between 51-73 db.

Keywords: Steganography, Encryption, LSBraille

1. INTRODUCTION

Communication through digital media has been progressing very rapidly, being able to connect access technology in the world to communicate and exchange information with the size of large messages in a relatively quick and easy. In some cases, messages or information exchange, the parties messaging want the message to avoid making illegal information and confidential, but not to arouse suspicion in the process of transmission of information even if they take advantage of the public path. To resolve this problem, steganographic techniques can be applied as a technique for data security.

According steganography is a technique for hiding information that is eternal in a container something that the result will look like any other normal information. Therefore, steganography chosen as a method to assist in the concealment of information. In the steganography using two different media simultaneously, where one medium that contains information and other media as an information carrier. Media information carrier can be shaped image, audio and video while the inserted media can be text, image and video , Lee and Chen [1].

Several studies have been conducted with a steganographic various methods. One of them carried out by Kamau, and Mwangi Kimani [2] by applying the method of Least Significant Bit (LSB) and select specific bits to be inserted with a secret

message for the embedding process the message. Thus resulting stego image has a message insertion is relatively low. Another study conducted by Padmasri and Surabi [3] by applying the method Spread Spectrum and explain this method to store messages as noise in the stego image. At the level of noise power is low, the message the image will not be detected by the human eye, while the noise at higher levels, noise appears as speckles

Some previous steganographic methods have a problem in storage capacity as well as the message and the resulting stego image. Ali [4] has answered this problem by Least Significant Braille method which is one method that is well within the message's safety. This method is expected to insert a secret message that have a bigger capacity and yield a better stego image.

From the above description, the authors will examine how to address the lack of message storage capacity and is able to produce a better image stego method Least Significant Braille (LSBraille).

2. ALGORITHM

His study uses a digital image file with bmp format as the image of a container to be inserted message. Prior to insertion of the message, the pixels of the image of the container changed first of pixels decimal form into binary form, because the message will be inserted into the channel bits into 8 channel blue, where each one character of a message has 6 bits and each one pixel can hold one bit.

2.1. ANALYSIS OF ALGORITHMS LIST SIGNIFICANT BRAILLLE

There are two steps in steganographic system is the process of hiding (embedding) and extraction of data from the image of the container. Concealment is done by replacing the bits of data in a segment of the image with the bits of confidential data. In the arrangement of bits in a byte (1 byte = 8 bits), there is the most significant bit (Most Significant Bit. or MSB) and the least significant bit (Least significant Bit or LSB). Bit suitable to be replaced is a bit Least Significant Bit, because the changes are just changes the value byte one higher or one lower than the previous value. Suppose the byte states red, then change one bit LSB does not change the red color significantly.

Braille method itself uses six bits of each of his characters, not 8 bits as they are used in the ASCII table. So by using this representation it can save 2 pixels of each process of embedding secret bits or more than a quarter of the maximum capacity of each image concealment cover. The process is carried out is divided into three phases, namely encryption and decryption process.

2.2. ANALYSIS OF ALGORITHMS LIST SIGNIFICANT BRAILLLE

To Insert the message on the digital image, the authors apply the method Least Significant Braille (LSBraille) by reading the pixels until the end of the digital image and then change the pixels - the pixels into binary form the next stage of the steps taken is to insert the character - the character of a secret message to in the blue channel in the image container. In the bitmap image in each pixel can insert one bit

ISSN: 2252-4274 (Print)
ISSN: 2252-5459 (Online)

of from each character. Then the formula of the number of characters is M x N / 6. Where, M = N = width and height. While 6 is the number of bits of each character.

A. Enkription Process

To Insert the message on the digital image, the authors apply the method Least Significant Braille (LSBraille) by reading the pixels until the end of the digital image and then change the pixels - the pixels into binary form the next stage of the steps taken is to insert the character - the character of a secret message to in the blue channel in the image container. In the bitmap image in each pixel can insert one bit of Daris each character. Then the formula of the number of characters is M x N / 6. Where, M = N = width and height. While 6 is the number of bits of each character.

A flow diagram of the process secret message insertion into the container's image is as follows

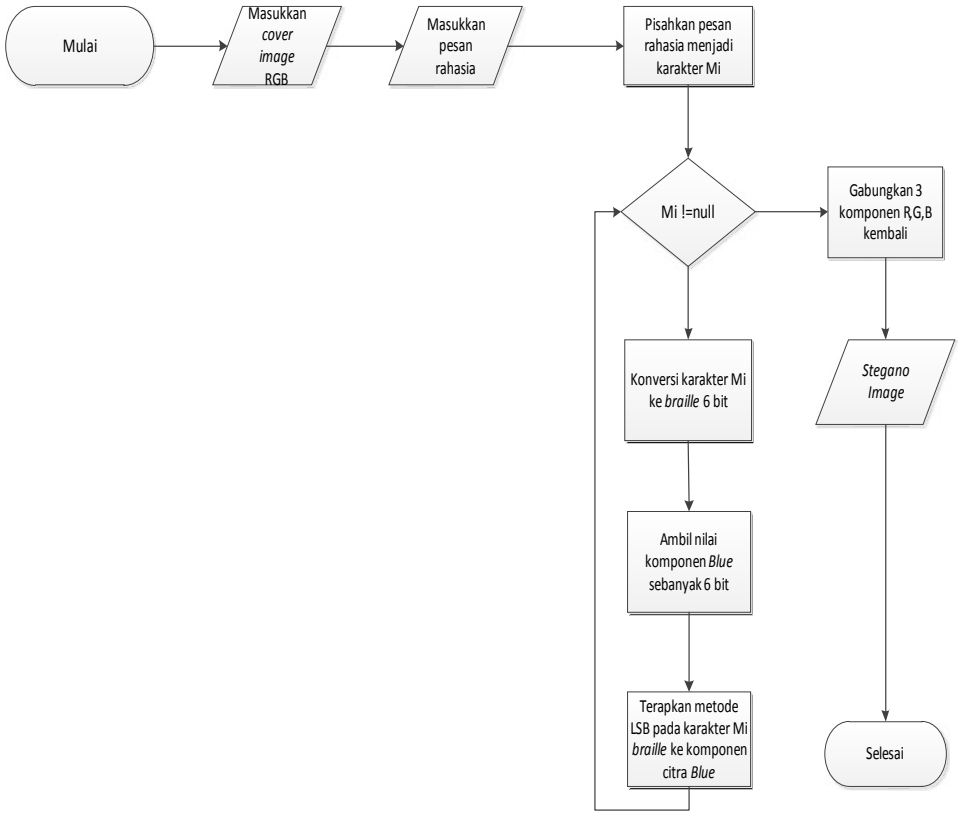

FIGURE 1. Insertion process messages with method LSBraille

Stages in the encryption processing scheme shown in Figure 1:

- Digital image'll enter * .bmp format 24 Bit.
- Then insert a secret message * .txt format that will be inserted into the cover image.
- Separate the secret message into a character M = {m1, m2 ...., Mn}.

- In his next process occurs initialization code secret message. If a character message! = Null then the process will continue into the conversion process a secret message to braille characters 6 bits, otherwise the process will be completed and will continue to process the merger of Red, Green, Blue became a whole pixel.
- During character message! = Null then the character will be a secret message in the converse i into braille method 6 bits.
- Color image'll enter * .bmp format 24 Bit.
- Then enter the secret message that will be inserted into the cover image.
- Separate the secret message into a character M = {m1, m2 ...., Mn}.
- In his next process occurs initialization code secret message. If a character message! = Null then the process will continue into the conversion process a secret message to braille characters 6 bits, otherwise the process will be completed and will continue to process the merger of Red, Green, Blue became a whole pixel.
- During character message! = Null then the character of the secret message will be converted into braille method 6 bits.
- Then take the blue component value by 6 bits to be inserted a secret message that is difficult in conversion into braille method.
- Apply the method of Least Significant Bit on the character of the message Mi to the image component Blue.
- Once the message has been inserted, combine 3 components Red, Green, Blue becomes a pixel back.
- Cover image 24 bit image already inserted message.

A. Decryption Process

In the extraction process secret message, the steps taken is to change first of all pixel values stego image into binary, where the binary values will be accommodated in one array and each 6 bits will be cut to be turned into a form of character through the database. The results of the extraction process will stop for an identification mark the end of a message.

3. EXPERIMENT AND RESULTS

Testing is being done with n order to determine the level of resistance stego image of the various processes the image and measure the level of accuracy results Peak Signal to Noise Ratio of stego image after inserting a message. Testing Resilience file stego image is done in order to determine whether a secret message that is in stego image file is still awake or not after the various processes on the image that stego image conversion, cropping, resampling, and rotation.

Original image files that have been inserted a secret message is cut in certain parts, then extracted a secret message to see if the message is still in the secret stego image file or not. The result if the cuts are made in the image pixels that holds the

ISSN: 2252-4274 (Print)
ISSN: 2252-5459 (Online)

message, the message disappears and if the cutting is performed not on the pixels that holds the message, then the message can still be extracted back

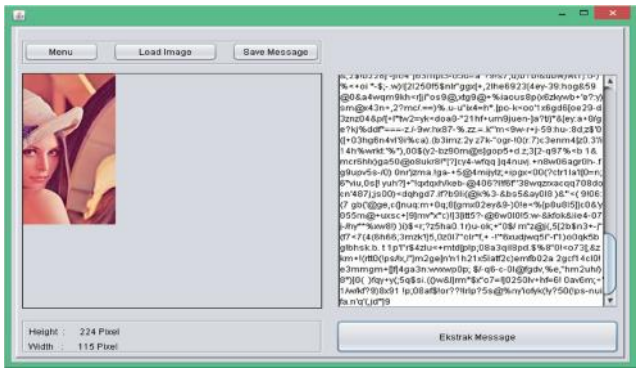

FIGURE 2. Testing cropping 'lrna.bmp'

Original image files that have been inserted a secret message is cut in certain parts, then extracted a secret message to see if the message is still in the secret stego image file or not. The result if the cuts are made in the image pixels that holds the message, the message disappears and if the cutting is performed not on the pixels that holds the message, then the message can still be extracted back. Figure 2 shows the test results lena cropping the image.

pada piksel yang menampung pesan, maka pesan masih bisa diekstrak kembali.

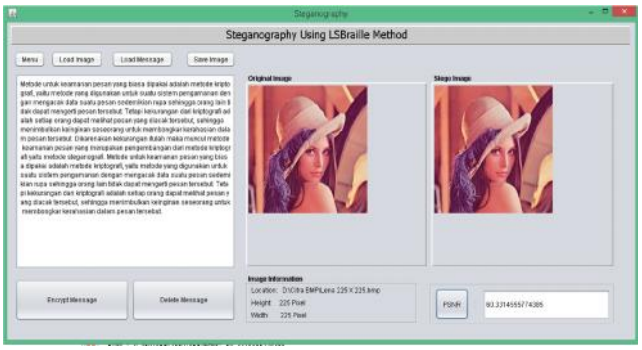

FIGURE 3. Testing PSNR

Figure 3 shows that the PSNR results of such file indicates a sizeable number, which means its PSNR value, in accordance with the Figure 3.

4. CONCLUSION

Inserted secret message is not resistant to a variety of digital image processing, because of the different extracted secret message with a secret message starting inserted after stego image file undergoing a process such as cropping, resampling, conversion, and compression. Comparison of the terms of the calculation of Peak Signal to Noise Ratio (PSNR) shows that between the original image and stego

image is almost the same so that the naked eye can not distinguish between the two images. The result of the calculation of PSNR value obtained from experiments on all data samples between 51-73 dB.

REFERENCES

[1]. Lee, Y. K and Chen, L. H. 2000. High Capacity Image Steganography model. IEEE Computer Security.

[2]. Kamau, G. M., Kimani, S., & Mwangi, W. 2012. An enhanced Least Significant Bit Steganographic Method for Information Hiding. Journal of Information Engineering and Applications, 2(9), 1-11.

[3]. Padmasri, B., & Surabi, M. Amutha. 2013. Spread Spectrum Image Steganography with Advanced Encryption Key Implementation. Journal of Advanced Research in Computer Science and Software Engineering Steganography Algorithm to Hide Secret Message Inside an Image Volume 3 (Page 713 – 720).

[4]. Ali, A. A. & Al-H. S. Saad. 2013. Image Steganography Technique By Using Braille Method of Blind People (LSBraille). International Journal of Image Processing (IJIP), Volume (7): Issue (1) (Page 81–88).

ISSN: 2252-4274 (Print)
ISSN: 2252-5459 (Online)